Data Loss Prevention

- History of Communications
  - Network Managers Meeting (Every Friday at 9AM)
    - May 2016
  - MT-ISAC
    - 1st presentation – July 2016
  - ITMC
    - August 2016

- November 21st 2016
  - DLP for SharePoint Online and OneDrive for Business was turned on/off

- Exchange – Audit mode on.
  - Estimated 1600 emails per day violate template. 400-500 emails per day are to/from external entities

- Conditions for Internal and External Rules
  - ABA Routing Number
  - Credit Card Number
  - Drug Enforcement Agency (DEA) Number
  - U.S. / U.K. Passport Number
  - U.S. Bank Account Number
  - U.S. Individual Taxpayer Identification Number (ITIN)
  - U.S. Social Security Number (SSN)
  - ~~MT Drivers License Number (DLN)~~

- Requirements for all conditions on internal rule
  - Minimum count = 10
  - Maximum count = unlimited
  - Minimum Confidence Level = 75%
    - DEA = 86%
  - Maximum Confidence Level = 100%

- Actions for all conditions on internal rule
  - Send notification email to:
    - The owner of the SharePoint site or OneDrive where the content is stored
    - The person who shared, emailed, or last modified the content
    - The owner of the SharePoint or the OneDrive content
    - Use the default email notification
    - Use default Policy Tip
    - Do not allow people to override the actions

- Incident Reports for internal rule
  - Use severity level High in reports
  - Incident reports include information about the item that was matched, where the match occurred, and the rules and policies it triggered. For email messages, the report also includes the message and the sensitive information that matched the rule.
    - The person who last modified the content
    - The types of content that matched rule
    - The rule's severity level

- Requirements for all conditions on external rule
  - Minimum count = 1
  - Maximum count = unlimited
  - Minimum Confidence Level = 75%
    - DEA = 86%
  - Maximum Confidence Level = 100%

- Actions for all conditions on external rule
  - Block people from sending email or accessing shared documents
    - If an email message or document contains sensitive information people won’t be able to send the message or access the message or access the document if it is shared
  - Send notification email to:
    - The owner of the SharePoint site or OneDrive where the content is stored
    - The person who shared, emailed, or last modified the content
    - The owner of the SharePoint or the OneDrive content
    - Use the default email notification
    - Use default Policy Tip
    - Do not allow people to override the actions

- Incident Reports for external rule
  - Use severity level High in reports
  - Incident reports include information about the item that was matched, where the match occurred, and the rules and policies it triggered. For email messages, the report also includes the message and the sensitive information that matched the rule.
    - The person who last modified the content
    - The types of content that matched rule
    - The rule’s severity level

- Sharing Outside the organization
  - Current setting:
    - Don’t allow sharing outside your organization
  - Suggested setting:
    - Allow users to invite and share with authenticated external users
  - Other possible settings:
    - Allow sharing only with the external users that already exist in your organization’s directory
    - Allow sharing to authenticated external users and using anonymous access links
  - Default link type
    - Suggested setting:
      - Direct – Only people who have permission
    - Other settings:
      - Internal – people in the organization only
      - Anonymous Access – anyone with the link

- Sharing Outside the organization
  - Additional Settings
    - Suggested settings:
      - External users must accept sharing invitations using the same account that the invitations were sent to
      - Prevent external users from sharing files, folders, and sites they don’t own
    - Other settings:
      - Limit external sharing using domains (applies to all future sharing invitations)
  - Notifications
    - E-mail OneDrive for Business owners when
      - Other users invite additional external users to shared files
      - External users accept invitations to access files

Action Items

- Approve the template
- Approve Implementation Starting January 17th.
  - DLP Turned on for SharePoint Online and OneDrive
  - OneDrive authenticated sharing to outside
  - Exchange – turn on in audit mode until July 1
    - Users would see tool tips and get notifications only. No blocking.

Conditions for Internal and External Rules

SharePoint and One Drive

External Block on 1

Internal Notify on 10

Exchange (Notify only until July 1)

External Notify on 1 (Block after July 1)

Internal Notify on 10

ABA Routing Number

Credit Card Number

Drug Enforcement Agency (DEA) Number

U.S. / U.K. Passport Number

U.S. Bank Account Number

U.S. Individual Taxpayer Identification Number (ITIN)

U.S. Social Security Number (SSN)

Need more “Live” testers for Exchange

  - Non-IT Staff
  - Real users

- For those who send sensitive info regularly – Use ePass Outlook Plug-In. Submit a ticket to SITSD ServiceDesk.

AT LEAST I'M NOT RESPONSIBLE FOR A DATA PROTECTION PROJECT...

The daydreams of cat herders...